A KTSI WHITE PAPER

INFORMATION ASSURANCE

RISK MANAGEMENT

“The Analytical Process & The Management Philosophy”

Frederick G. Tompkins

April 2000

ABSTRACT

Charles Mingus noted that: "Making the simple complicated is commonplace; making the complicated simple, awesomely simple, that's creativity." The purpose of this KTSI White Paper is to provide the reader with a straight forward no nonsense understanding of information assurance risk management. Information assurance risk management can be viewed in terms of performing risk analytical studies and implementing a risk-based information assurance program. This paper provides a description of the six phases of the analytical process and the steps necessary to implement a risk-based information assurance program.

BACKGROUND

The rapid explosion of the Internet and the associated electronic business applications when combined with the geometric (sometimes exponential) rate of technology change in information technology presents organizations with an environment that significantly increases the degrees of uncertainty. In "An Anatomy of Risk" William D. Rowe[1] introduces the concept of risk as follows:

> "The only certainty in life is death; uncertainty lies in when and how death occurs and whether it is final. Man strives to delay its onset and extend the quality of life in the interim. Threats to these objectives involve risks, some natural, some man-made, some beyond our control, and some controllable."

Risk management is about reducing uncertainty. Management is about making decision in the face of uncertainty. The more valid information management has at its disposal, the more valid decisions will be about the future. The author's corollary to Rowe's observation is:

> "There are two uncertainties in life: death and change. Death may or may not be the ultimate change depending upon your "religious" beliefs.

The major issue facing most of us in the information technology and information assurance fields is how to assure a reasonable level of comfort in the face of constant change. Due to rapid rates of change in technology and the applications of that technology what we are striving for is to be more comfortable in the short term than we are at the moment. To some degree, our level of comfort must be based on having the best information available about our environment, the things that can cause harm to that environment, our degree of vulnerability to the things that can cause harm, and the consequences to our organization in the event our vulnerabilities are exploited by the things that can cause harm. While there are no certainties that the steps we take to mitigate vulnerabilities will ensure that bad things do not happen, we can take reasonable

[1] Rowe, William D., *An Anatomy of Risk*, John Wiley and Sons, Inc., 1977.

steps to reduce the likelihood that consequences will be intolerable. In other words, we want and should be capable of, reducing risks to acceptable levels of tolerance.

One of the first steps in developing an understanding of our risk environment is to understand the effects of technology change. In the private, and to some extent, in the public sector, we are dealing with a new set of realities that the author likes to refer to as the "Now" Problem".[2],[3]

The "Now" problem is characterized by the following:

- We will live with commercial-off-the-shelf (COTS) products for the foreseeable future.
- We must contend with a high rate of technology change.
- We must operate at the "speed of business".
- We must accept some level or risk.

Commercial-Off-The-Shelf Products

There are several general security concerns about COTS products. From an end-user, consumer point of view COTS products tend to be generic solutions for non-specific problems - and every problem we have is unique. As a result many of us will be required to write bridge or conversion code to make a suite of products that will solve our unique problem. In addition, the COTS development process is one over which we as end users or consumers have little or no ability to affect the design, development or testing of the product. If we are a part of the advanced Beta test pool, the product is probably already "shrink wrapped" and on the shelf. The bottom line question then is how do we as end users know that the product performs as advertised, does only what it is intended to do - no more or no less, and provides an appropriate degree of security.

Rate of Technology Change

We are living in a world of unbelievable technology change - and the rate of change seems to keep increasing. In the 1982/3 time frame - about the time of the major introduction and adoption of the personal computer - the ½ life of technology was about 5 years. Today the ½ life of technology is about 5-6 months (maybe less in some instances). The major impact of this rate of change is that much of the technology becomes obsolete before we really figure out how to use or the use becomes common practice.

[2] Tompkins, Frederick G., *Information Assurance Seminar Game ICSA – Corporate Viewpoint,* U. S. Army War College, 1998.

[3] Tompkins, Frederick G.; *ICSA Approach to Certification: A Paradigm Shift for Information Security;* ICSA News, Carlisle, PA, August 1997; p. 9-13.

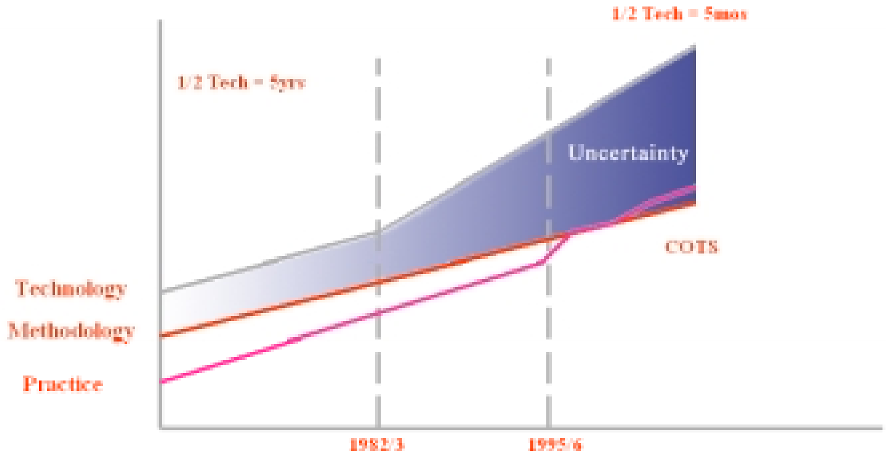

Figure 1. Implications of the Rate of Technology Change

This significant reduction in the ½ life of technology and the rate of technology change has caused us to compress our planning timeframes as indicated in the chart below:

	Historically	Currently
Strategic Planning	3-5 Years	8 Months
Tactical Planning	1-3 Years	30 Days
Operational Planning	1-12 Months	48-96 Hours

Figure 1. Compression of Planning Timeframes

The rapid rate of technology change that we are experiencing and the reliance on COTS means that uncertainty about our IT environment is increasing as well.

Speed of Business

The commercial world is a highly competitive arena. It is one in which bringing the best product or service to market in the most expedient time frame is absolutely essential. This approach is often referred to as "moving at the speed of business." Perhaps a better way of expressing this process is the inventory concept referred to as "just in time." Just in time refers to an inventory management process, which is designed to reduce warehousing of large quantities of goods that may occupy space for some time before they are utilized. A "just in time" approach requires critical scheduling, inventory control, and ordering that puts the parts or merchandise at the manufacturing site or the retail store coincident with the anticipated need for the item. An appropriate example is the recently opened Chrysler automobile manufacturing plant in South America where parts arrive approximately two hours before insertion in to a vehicle on the assembly line.

Risk Management

In general, the commercial world makes decisions based on a risk management basis. The primary basis for business decisions is the affect on the bottom line (profitability, shareholders, market share, etc.). Decisions must be based on a cost-benefit understanding that some degree of risk must be accepted. The government has tended to follow a practice of risk avoidance based on postulated or perceived threat and attempts to mitigate all vulnerabilities.

THE RISK MANAGEMENT ANALYTICAL PROCESS

The analytical process consists of six related but distinct phases:

- Risk Analysis
- Risk Reduction Analysis
- Management Decision
- Risk Reduction Planning
- Implementation and Maintenance of Safeguards
- Review and Audit

Risk Analysis

The focus of this data collection and analytic phase is to develop and document an understanding of what is at risk (assets and resources); what are the bad things that can happen to those assets; what are the vulnerabilities that could exploited to cause undesirable consequences; what safeguards are in place that could reduce the likelihood that undesirable consequences will occur; and some measurement of the potential consequences if the vulnerabilities are exploited.

Risk Reduction Analysis

The purpose of this phase is to identify safeguards that can be implemented to mitigate the vulnerabilities identified in the risk analysis; determine the operational feasibility of those safeguards relative to the technical and organizational environment; and, perform an economic feasibility of those safeguards. The technical, operational, and economic feasibility studies are used to provide a set of recommendations or alternatives to management that identify where unacceptable risks can be reduced to acceptable levels.

Management Decision

The risk analyst can identify the information assurance risks and what can be done to reduce risks. Management decides which of the recommendations or alternatives will implemented and allocates the resources for the purchase, design, development and implementation of safeguards.

Risk Reduction Planning

The purpose of this phase is to develop risk reduction plans that outline the tasks to be performed based on the direction received from management. The tasks should include identification of the safeguards, assignment of responsibility for design and development or acquisition, and the implementation of the safeguards.

Implementation and Maintenance of Safeguards

This phase involves the installation, operation, and maintenance of the new or modified safeguards. Depending on the type of safeguards some training of personnel may be involved and coordination of changes of operational procedures with the affected personnel and organizational entities. Maintenance procedures and help desk procedures may be required. In the case of software implementations, procedures for updates and new versions will be needed.

Review and Audit

Changes in the technology or operational environment will occur. New threats and vulnerabilities will affect the overall security posture. To assure that the security posture remains within acceptable risk tolerances, periodic reassessments will be required. Before the introduction of new technology, assessments should be performed to determine the potential affects on the environment, both technologically and operationally.

RISK MANAGEMENT & INFORMATION ASSURANCE PROGRAMS

There are two fundamental approaches to developing, implementing and operating an Information Assurance program: the compliance-based approach[4] and the risk-based approach.

A prime example of the compliance-based approach is the highly and centrally controlled, structured program whose procedures are intricate and rigidly enforced for every user. This is the approach historically used by the U.S. Department of Defense.

[4] National Aeronautics and Space Administration; *Johnson Space Center Automated Information Systems Security Manual*; October 1992; p. 1-3 – 1-4.

Compliance-based programs yield clear requirements for protecting national security information. Although such programs are easy to audit, there some notable disadvantages:

a. A compliance-based approach treats every system the same. All systems must protect against the same threats, whether they exist or not.
b. A compliance-based approach eliminates the flexibility of the line manager who controls and processes the information to make reasonable decisions about risk acceptability.
c. A compliance-based approach may result in the implementation of unnecessary controls resulting in unnecessary expenditure of dollars and personnel resources.
d. A compliance-based approach does not respond well to rapid changes in technology.

A risk-based approach to Information Assurance is intended to place the responsibility for determining the actual threats to a processing environment and determining how much risk to accept, in the hands of the line managers who are most familiar with the environment in which they operate. The risk-based approach requires each system or application manager to understand the threats and vulnerabilities peculiar to his or her environment so that the risks may be identified. Each manager then evaluates alternatives so the cost-effective decisions may be made with respect to budget and processing realities inherent to each case.

Ultimately, it is the organizational senior management that is responsible for assuring that all information technology resources are appropriately protected consistent best practices and due diligence (or State/Federal policy requirements within their respective operating environments). To provide a baseline set of guidelines applicable to whole communities, senior management should determine that certain types of controls are required to establish a minimum level of acceptable risk across the entire enterprise.

The focus of an Information Assurance Program is not to eliminate risk but to provide a sound and logical methodology, consistent with good systems engineering, by which risks can be managed. Once risks are assessed and ranked by priority, they can be reduced during the normal course of business. Information assurance should not be a separate endeavor; it is a process that should be integrated into an application's or system's life cycle.

There are nine components of a risk-based Information Assurance Program:

- Policy
- Assignment of Responsibilities
- Procedures and Guidelines
- Systems Engineering Process
- Information Technology

- Personnel Security
- Awareness And Training
- Incident Response
- Management Review

Policy

Policy is a statement by the senior management of an organization of what is expected within the organization. The policy should not include how the expectation is to be discharged or how success is measured.

Assignment of Responsibilities

The next step is to identify who is responsible for policy implementation. The primary players will include:

- Chief Executive/Operating Officer
- Chief Information Officer
- Chief Financial Officer
- Information Systems Security Manager
- Operating Element Management
- System/Data Managers/Owners
- Users

Procedures and Guidelines

Procedures and guidelines define methodological approaches for accomplishing the activities required to implement and maintain the Information Assurance Program. Procedures and guidelines should include the following areas:

- **Systems Engineering Process**

  Procedures or guidelines should be established for identifying data and applications based on criticality or sensitivity; assuring that security requirements are defined during the functional requirements definition of the systems life cycle process; defining testing approaches for security requirements; and, the steps in maintaining security controls throughout the life of the system.

- **Information Technology**

  Procedures or guidelines should be established to assure that Information Technology management is cognizant of the sensitivity/criticality and the security requirements that must be implemented in the IT infrastructure to adequately protect the applications and associated data. The procedures or guidelines should identify a process for assessing the security risks within the IT infrastructure and for developing, maintaining and testing disaster response and recovery plans.

- **Personnel Security**

  Procedures should be established for performing background checks on personnel based on their roles within the organization, degree of access to sensitive or critical data or systems, and ability to develop or implement changes in the IT infrastructure or systems. The procedures should include requirements for periodic screening, auditing, reporting or unacceptable actions by personnel, and an adjudication process.

- **Awareness and Training**

  Procedures or guidelines should be established for assuring that all personnel in the organization are aware of the need for Information Assurance and the vulnerabilities associated with information technology systems. Training processes should be implemented to assure that personnel know how to mitigate the vulnerabilities relative to their job responsibilities.

- **Incident Response**

  Procedures or guidelines should be established that define what constitutes a security incident, the steps to be accomplished upon discovery and the appropriate reporting chains. Procedures should include the data to be reported or collected relative to the incident. Monitoring processes and auditing activities should be identified.

- **Management Review**

  In a risk-based Information Assurance Program, senior management allocates the risk decisions for operational entities and systems. However, senior management is still ultimately responsible and accountable and should review the process by which risk decisions are made. Therefore, a management review process should be implemented to include periodic review, evaluation and reporting of the organizational Information Assurance Program activities. The reviews should include periodic review of security plans, training programs, and auditing and testing of the security posture of systems.

SUMMARY

Risk management consists of both analytical and a management processes. The analytical process assures that an organization develops an understanding of its information technology infrastructure security posture, which risks are acceptable, what steps can be taken to reduce unacceptable risks to an acceptable level in a cost effective manner. The management process provides the infrastructure to assure that risk decisions are made by those closest to the systems and technology and provides an appropriate level of senior management oversight and review.